UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,068	04/09/2004	Jung-Soo Jung	678-1443	2064

66547 7590 11/01/2007

THE FARRELL LAW FIRM, P.C.
333 EARLE OVINGTON BOULEVARD
SUITE 701
UNIONDALE, NY 11553

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
11/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/822,068	JUNG ET AL.	
	Examiner	Art Unit	
	Oscar A. Louie	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/04/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-14 and 16-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7, 9-14, & 16-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 09/04/2007. The examiner acknowledges the applicant's amendments and arguments and hereby withdraws his 35 U.S.C. 112 2nd paragraph rejections regarding Claims 3-9, 13-17, 19, 20, 22, 24-27, 31, & 34-36. The cancellation of Claims 8 & 15 have also been noted. Claims 1-7, 9-14, & 16-36 are pending and have been considered as follows.

Claim Objections

1. Claims 1, 9, & 17 are objected to because of the following informalities:
   - Claim 1 line 3 recites, "the mobile station" which should be "...a mobile station..."
   - Line 5 of Claims 9 & 17 recite, "the mobile station" which should be "...a mobile station..."

   Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1, 17, 20, & 31 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- Claims 1, 17, 20, & 31 recite "different encryption information" and although the specification provides support for "predetermined encryption information," there does not appear to be support for the amended subject matter.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-7, 9-14, & 16-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jobst et al (US-6707915-B1).

Claim 1:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, but do not explicitly disclose,

- "generating a registration message including a predetermined registration identifier for identification of the encryption information"
- "transmitting the generated registration message to a base station"
- "receiving updated encryption information for decryption of the broadcast data from the base station"
- "when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station"
- "updating the registration identifier based on the updated encryption information"

however, Jobst et al do disclose,

- "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58];
- "transfers a message to the providing communication terminal" [column 1 lines 56-57];
- "the binary code 44 (the code image) of the file and the calculated first digital signature 43 (sig2) to the requesting phone" [column 7 lines 55-57];
- "Based on the binary code 47 (the code image) and the phone password 45 the phone 1 starts to calculate a second signature" [column 8 lines 9-11];

- "The output from the signature generating algorithm 42 may be regarded as a first digital signature 43 (sig2) that is unique for the this specific software transfer, as it is based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code" [column 7 lines 48-52];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "generating a registration message including a predetermined registration identifier for identification of the encryption information" and "transmitting the generated registration message to a base station" and "receiving updated encryption information for decryption of the broadcast data from the base station" and "when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station" and "updating the registration identifier based on the updated encryption information," in the invention as disclosed by Jobst et al since prior to the transmission of a message from a mobile device to a base station, it must be created (i.e. generated) otherwise there would be nothing to send. In addition, multiple digital signatures may be used in the process of validation and decryption of information where a second digital signature may be based on some aspect of the first digital signature. Also, the transmission of updated encryption information would be necessary and is implied with each new transaction requiring new digital signatures.

Claim 2:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, as in Claim 1 above, further comprising,

- "at least one of a predetermined mask key required for decryption of the broadcast data" (i.e. "The two signatures 43 and 46 are calculated base on the very same secure hash algorithm 42 (MD5). By comparing these two signatures 43 and 46 the phone 1 can prove the validity of the received message") [column 10 lines 58-61].
- "generation information for the mask key" (i.e. "The output from the signature generating algorithm 42 may be regarded as a first digital signature 43 (sig2) that is unique for the this specific software transfer, as it is based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code") [column 7 lines 48-52].
- "a lifetime of the mask key" (i.e. "When the two signatures 43 and 46 are different this may be caused by errors in the transmission. Then steps 201-208 are repeated. If the re-transmission is also unsuccessful the phone may automatically inform the service provider about the situation and desist from further attempts") [column 11 lines 17-22].

Claim 3:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, as in Claim 2 above, further comprising,

- "the registration identifier includes a hash value determined by applying a hash function to a corresponding mask key each time the mask key is updated" (i.e. "the phone password 40 may be calculated by means of a per se known secure hash algorithm, such as MDS from the RSA Data; Security Company. The MD5 algorithm 39 that is a secure hash algorithm, receives the IMEI code 37 and the Master Password 38 from the memories associated with the certification center 35, and outputs a Phone Password 40 in response") [column 7 lines 25-32].

Claim 4:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, as in Claim 2 above, further comprising,

- "the registration identifier includes a sequence number sequentially assigned to a corresponding mask key each time the mask key is updated" (i.e. "a sequence specific for the receiving phone and a sequence specific for the transmitted software code") [column 7 lines 50-51].

Claim 5:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, as in Claim 1 above, further comprising,

- "the registration message is a message that is transmitted from the mobile station to the base station for a predetermined time while the mobile station is using a broadcast service" (i.e. "When the two signatures 43 and 46 are different this may be caused by errors in the transmission. Then steps 201-208 are repeated. If the re-transmission is also unsuccessful the phone may automatically inform the service provider about the situation and desist from further attempts") [column 11 lines 17-22].

Claim 6:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, as in Claim 1 above, further comprising,

- "the encryption information is generated by a packet data service node and transmitted to the mobile station via the base station" (i.e. " The invention relates to a new method for transferring a data packet, e.g. a software sequence, between two communication terminals") [column 1 lines 8-10].

Claim 7:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, as in Claim 1 above, further comprising,

- "the encryption information is generated by the base station and transmitted to the mobile station" (i.e. "the service provider 33 starts to transfer the binary code 44 (the code image) of the file and the calculated first digital signature 43 (sig2) to the requesting phone") [column 7 lines 54-57].

Claim 9:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, but do not explicitly disclose,

- "receiving a registration message transmitted from the mobile station"
- "determining whether a registration identifier for identification of encryption information required for decryption of broadcast data is included in the registration message"
- "determining whether it is necessary to transmit updated encryption information to the mobile station"
- "transmitting the updated encryption information to the mobile station according to the determination result"
- "when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station"

however, Jobst et al do disclose,

- "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58];

- "said providing communication terminal includes means for verifying the validity of the first unique identification code, and means for transmitting a message, upon a successful verification, to the requesting communication terminal, said message includes the requested data packet and a second unique identification code; said requesting communication terminal comprises means for verifying the validity of the second unique identification code" [column 3 lines 9-15];
- "Hereby the software provider will have an opportunity to check whether the requesting phone will be allowed to receive the requested data packet" [column 4 lines 31-34];
- "In order to secure that only authenticated additional software is downloaded into to a phone. This additional software need to be verified for the following: 1. The software originated from a reputable source and can be expected to be well-behaved." [column 4 lines 35-39];
- "The output from the signature generating algorithm 42 may be regarded as a first digital signature 43 (sig2) that is unique for the this specific software transfer, as it is based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code" [column 7 lines 48-52];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "receiving a registration message transmitted from the mobile station" and "determining whether a registration identifier for identification of encryption information required for decryption of broadcast data is included in the registration message" and "determining whether it is necessary to transmit updated encryption information to the mobile station" and "transmitting the updated encryption information to the mobile station

according to the determination result" and "when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station," in the invention as disclosed by Jobst et al since the base station would have to receive a transmission from a mobile device in order to authenticate and determine whether it is valid. In addition, there would only be two results of an authentication verification. The first being if the mobile device is invalid than there would be no reason to provide encryption information to it. The second being if the mobile device is valid, then permit further functionality. Also, the transmission of updated encryption information would be necessary and is implied with each new transaction requiring new digital signatures.

Claim 10:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, as in Claim 9 above, further comprising,

- "at least one of a predetermined mask key required for decryption of the broadcast data" (i.e. "The two signatures 43 and 46 are calculated base on the very same secure hash algorithm 42 (MD5). By comparing these two signatures 43 and 46 the phone 1 can prove the validity of the received message") [column 10 lines 58-61].
- "generation information for the mask key" (i.e. "The output from the signature generating algorithm 42 may be regarded as a first digital signature 43 (sig2) that is unique for the this specific software transfer, as it is based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code") [column 7 lines 48-52].

- "a lifetime of the mask key" (i.e. "When the two signatures 43 and 46 are different this may be caused by errors in the transmission. Then steps 201-208 are repeated. If the re-transmission is also unsuccessful the phone may automatically inform the service provider about the situation and desist from further attempts") [column 11 lines 17-22].

Claim 11:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, as in Claim 10 above, further comprising,

- "the registration identifier includes a hash value determined by applying a hash function to a corresponding mask key each time the mask key is updated" (i.e. "the phone password 40 may be calculated by means of a per se known secure hash algorithm, such as MDS from the RSA Data; Security Company. The MD5 algorithm 39 that is a secure hash algorithm, receives the IMEI code 37 and the Master Password 38 from the memories associated with the certification center 35, and outputs a Phone Password 40 in response") [column 7 lines 25-32].

Claim 12:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, as in Claim 10 above, further comprising,

- "the registration identifier includes a sequence number sequentially assigned to a corresponding mask key each time the mask key is updated" (i.e. "a sequence specific for the receiving phone and a sequence specific for the transmitted software code") [column 7 lines 50-51].

Claim 13:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, as in Claim 9 above, further comprising,

- "performing an accounting process on the mobile station through a packet data service node when the base station transmits updated encryption information to the mobile station" (i.e. "requesting communication terminal transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code identifying the requesting communication terminal; said providing communication terminal verifies the validity of the first unique identification code, and upon a successful verification, responds by transferring a message to the requesting communication terminal including the requested data packet and a second unique identification code; and said requesting communication terminal verifies the validity of the second unique identification code, and upon a successful verification, stores the data packet accordingly") [column 1 lines 55-67].

Claim 14:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, as in Claim 9 above, further comprising,

- "holding a current state of the mobile station for a predetermined lifetime of the encryption information when the registration identifier of the mobile station is identical to a registration identifier available in the base station" (i.e. "If these two signatures 43 and 46 fit together that is are identical the phone 1 deems the response message to be coming from an authorized software provider having access to the Master Password 38. Therefor the phone 1 deems the received code image to be authentic and starts to transfer the down loaded code 31 to the MT software") [column 8 lines 20-25].

Claim 16:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, as in Claim 9 above, further comprising,

- "transmitting a predetermined response message to the mobile station in response to the registration message if it is determined that transmission of the updated encryption information is not necessary" (i.e. "If the user does not have a valid account a reject message is sent to the user in step 104 where the user is informed about the situation") [column 9 lines 38-40].

Claim 17:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, but do not explicitly disclose,

- "generating a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data"
- "transmitting the generated registration message to a base station while the mobile station is using a broadcast service"
- "receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit"

however, Jobst et al do disclose,

- "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58];
- "transfers a message to the providing communication terminal" [column 1 lines 56-57];
- "the binary code 44 (the code image) of the file and the calculated first digital signature 43 (sig2) to the requesting phone" [column 7 lines 55-57];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "generating a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data" and "transmitting the generated registration message to a base station while

the mobile station is using a broadcast service" and "receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit," in the invention as disclosed by Jobst et al since prior to the transmission of a message from a mobile device to a base station, it must be created (i.e. generated) otherwise there would be nothing to send. In addition, multiple digital signatures may be used in the process of validation and decryption of information where a second digital signature may be based on some aspect of the first digital signature..

Claim 18:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, as in Claim 17 above, further comprising,

- "generating another registration message for requesting a new mask key" (i.e. "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58].
- "transmitting the generated registration message to the base station if the lifetime of the mask key has expired" (i.e. "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58].

Claim 19:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, but do not explicitly disclose,

- "receiving a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data, from the mobile station"
- "analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key"
- "transmitting the encryption information to the mobile station when the base station determines to transmit the encryption information"

however, Jobst et al do disclose,

- "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58];
- "Hereby the software provider will have an opportunity to check whether the requesting phone will be allowed to receive the requested data packet" [column 4 lines 31-34];
- "In order to secure that only authenticated additional software is downloaded into to a phone. This additional software need to be verified for the following: 1. The software originated from a reputable source and can be expected to be well-behaved." [column 4 lines 35-39];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "receiving a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data, from the mobile station" and "analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key" and "transmitting the encryption information to the mobile station when the base station determines to transmit the encryption information," in the invention as disclosed by Jobst et al since a base station transmitting a message to a communication terminal (i.e. mobile station) would have to be received in order to authenticate the communication terminal. In addition, the analysis of various conditions of data (i.e. values, keys, certificates, signatures, etc) is typical for multi-tiered/layered authentication procedures. Lastly, the transmission of encryption/decryption information to a mobile station would commonly only occur after a verification has been made to ensure security.

Claim 20:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, but do not explicitly disclose,

- "generating a registration message for use of a broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires"

- "receiving the current encryption information and next encryption information including their lifetimes from the base station in response to the registration message"
- "continuously decrypting the broadcast data using the next encryption information when the lifetime of the current encryption information expires"

however, Jobst et al do disclose,

- "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58];
- "Hereby the software provider will have an opportunity to check whether the requesting phone will be allowed to receive the requested data packet" [column 4 lines 31-34];
- "In order to secure that only authenticated additional software is downloaded into to a phone. This additional software need to be verified for the following: 1. The software originated from a reputable source and can be expected to be well-behaved." [column 4 lines 35-39];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "generating a registration message for use of a broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires" and "receiving the current encryption information and next encryption information including their lifetimes from the base station in response to the registration message" and "continuously decrypting the broadcast data using the next encryption information when the lifetime of the current encryption information expires," in the invention as disclosed by Jobst et al since prior to the transmission of a message it must be generated and may be generated with different types of data (i.e. unique identification

information, etc). The aspect of time constraints on the connection (i.e. encryption information) is typical of data communications. That is, a connection should not sit idle forever or permit unlimited access to resources. In addition, a base station transmitting a message to a communication terminal (i.e. mobile station) would have to be received in order to authenticate the communication terminal. It is noted that the examiner considers it immaterial for a mobile station to continuously decrypt broadcast data when the lifetime of the current encryption information expires, since it is obvious for a terminal (i.e. mobile station) to continuously use the existing encryption/decryption information to decrypt data unless otherwise informed of an encryption key change.

Claim 21:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, a method for receiving a broadcast service in the mobile station, as in Claim 20, further comprising,

- "the predetermined skew time is set to a time longer than a maximum period among registration message transmission periods of all mobile stations receiving a broadcast service in a service area of the base station" (i.e. "the phone starts to wait (step 204) for the response message") [column 10 lines 39-40].

Claim 22:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, but do not explicitly disclose,

- "receiving a registration message for use of a broadcast service by the mobile station"
- "transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires"

however, Jobst et al do disclose,

- "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58];
- "In order to secure that only authenticated additional software is downloaded into to a phone. This additional software need to be verified for the following: 1. The software originated from a reputable source and can be expected to be well-behaved." [column 4 lines 35-39];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "receiving a registration message for use of a broadcast service by the mobile station" and "transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires," in the invention as disclosed by Jobst et al since a base station

transmitting a message to a communication terminal (i.e. mobile station) would have to be received in order to authenticate and verify the communication terminal, prior to the transmission of encryption/decryption information.

Claim 23:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, as in Claim 22 above, further comprising,

- "the skew time is set to a time longer than a maximum period among registration message transmission periods of all mobile stations receiving broadcast service in a service area of the base station" (i.e. "the phone starts to wait (step 204) for the response message") [column 10 lines 39-40].

Claim 24:

Jobst et al disclose, in a mobile communication system for providing a broadcast service to a plurality of mobile stations over a radio channel, a method for providing by a base station a broadcast service to the mobile station, but do not explicitly disclose,

- "receiving a predetermined registration message for use of a broadcast service by the mobile station"
- "transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires"

however, Jobst et al do disclose,

- "transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code" [column 1 lines 56-58];
- "In order to secure that only authenticated additional software is downloaded into to a phone. This additional software need to be verified for the following: 1. The software originated from a reputable source and can be expected to be well-behaved." [column 4 lines 35-39];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "receiving a predetermined registration message for use of a broadcast service by the mobile station" and "transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires," in the invention as disclosed by Jobst et al since a base station transmitting a message to a communication terminal (i.e. mobile station) would have to be received in order to authenticate and verify the communication terminal, prior to the transmission of encryption/decryption information..

Claim 25:

Jobst et al disclose, in a mobile communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, but do not explicitly disclose,

- "transmitting, by the mobile station, a first registration message for initial use of a broadcast service to the base station"
- "upon receiving the first registration message, transmitting by the base station encryption information for decryption of broadcast data to the mobile station"
- "upon receiving the encryption information, generating by the mobile station a registration identifier which includes identification information of the encryption information"
- "generating by the mobile station a second registration message including the registration identifier"
- "transmitting the generated second registration message to the base station if second or later registration for use of the broadcast service by the mobile station is required"
- "comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station"
- "transmitting updated encryption information to the mobile station"

however, Jobst et al do disclose,

- "transfers a message to the providing communication terminal" [column 1 lines 56-57];
- "When the certification center 35 has calculated the first digital signature 43 (sig2) the service provider 33 starts to transfer the binary code 44 (the code image) of the file and the calculated first digital signature 43 (sig2) to the requesting phone" [column 7 lines 53-57];

- "When the phone 1 receives a binary code 47 and the first digital signature... the phone password 45 is stored as a part of the MT software 30 in the phone 1. The phone password 45 is granted by the software provider 33 when an account is established" [column 7 lines 62-67 & column 8 line 1];
- "Based on the binary code 47 (the code image) and the phone password 45 the phone 1 starts to calculate a second signature" [column 8 lines 9-11];
- "Further to the verification of the authorization of the received code the described method provides the added benefit that the transmission of the received code has been free of errors. This is due to the fact that the code image is used for the calculation of the signatures (sig2 and sig2') 43 and 46" [column 8 lines 27-32];
- "If these two signatures 43 and 46 fit together that is are identical the phone 1 deems the response message to be coming from an authorized software provider" [column 8 lines 20-22];
- "When the certification center 35 has calculated the first digital signature 43 (sig2) the service provider 33 starts to transfer the binary code 44 (the code image) of the file and the calculated first digital signature 43 (sig2) to the requesting phone" [column 7 lines 53-57];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "transmitting, by the mobile station, a first registration message for initial use of a broadcast service to the base station" and "upon receiving the first registration message, transmitting by the base station encryption information for decryption of broadcast data to the mobile station" and "upon receiving the encryption information, generating by the mobile

station a registration identifier which includes identification information of the encryption information" and "generating by the mobile station a second registration message including the registration identifier" and "transmitting the generated second registration message to the base station if second or later registration for use of the broadcast service by the mobile station is required" and "comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station" and "transmitting updated encryption information to the mobile station," in the invention as disclosed by Jobst et al since typically a phone (i.e. mobile station) initiates authentication with a providing communication terminal (i.e. base station) and may send various forms of authentication information (i.e. encryption/decryption information, unique identifiers, keys, certificates, signatures, etc). The mobile station typically would generate information to send to the base station, which in turn would perform it's own calculations and generate information in response to the mobile station. A "second registration message" could be verification values or some other form of verification/validation that further ensures a successful authentication and non-disrupted communication. Often times these verification values could be checksums or some other coded information that when calculations are performed upon them (i.e. hashing), return the same result to both the base station and mobile station, validating their communications.

Claim 26:

Jobst et al disclose, in a mobile communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 25 above, further comprising,

- "requesting by the base station an accounting process on the mobile station through the packet data service node if the registration identifiers are different" (i.e. "requesting communication terminal transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code identifying the requesting communication terminal; said providing communication terminal verifies the validity of the first unique identification code, and upon a successful verification, responds by transferring a message to the requesting communication terminal including the requested data packet and a second unique identification code; and said requesting communication terminal verifies the validity of the second unique identification code, and upon a successful verification, stores the data packet accordingly") [column 1 lines 55-67].

Claim 27:

Jobst et al disclose, in a mobile communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 25 above, further comprising,

- "holding by the base station the current encryption information of the mobile station" (i.e. "The phone password 45 is granted by the software provider 33 when an account is established") [column 7 line 67 & column 8 line 1].
- "deferring an accounting process on the mobile station if the registration identifiers are identical" (i.e. "The phone password 40 calculated by the software provider 33 is identical with the phone password 45 granted to the phone. The two passwords 40 and 45 differ only when errors occur in the calculation at the software provider") [column 8 lines 1-8].

Claim 28:

Jobst et al disclose, in a mobile communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 25 above, further comprising,

- "the encryption information includes at least one of a predetermined mask key required for decryption of the broadcast data" (i.e. "The phone password 45 is granted by the software provider 33 when an account is established") [column 7 line 67 & column 8 line 1].
- "generation information for the mask key" (i.e. "If the certification center 35 deems the request message 36 to be valid the certification center 35 then calculates a phone password 40. According to the preferred embodiment the phone password 40 may be calculated by means of a per se known secure hash algorithm") [column 7 lines 24-28].
- "a lifetime of the mask key" (i.e. "Otherwise the phone skips the received software (code image 47) and asks for a re-transmission in step 209. When the two signatures 43 and 46 are different this may be caused by errors in the transmission. Then steps 201-208 are repeated. If the re-transmission is also unsuccessful the phone may automatically inform the service provider about the situation and desist from further attempts") [column 11 lines 16-22].

Claim 29:

Jobst et al disclose, in a mobile communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 28 above, further comprising,

- "the registration identifier includes a hash value determined by applying a hash function to a corresponding mask key each time the mask key is updated" (i.e. "If the certification center 35 deems the request message 36 to be valid the certification center 35 then calculates a phone password 40. According to the preferred embodiment the phone password 40 may be calculated by means of a per se known secure hash algorithm") [column 7 lines 24-28].

Claim 30:

Jobst et al disclose, in a mobile communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 28 above, further comprising,

- "the registration identifier includes a sequence number sequentially assigned to a corresponding mask key each time the mask key is updated" (i.e. "The output from the signature generating algorithm 42 may be regarded as a first digital signature 43 (sig2) that is unique for the this specific software transfer, as it is based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code") [column 7 lines 48-52].

Claim 31:

Jobst et al disclose, a broadcast service system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, but do not explicitly disclose,

- "at least one mobile station connected to the base station through the radio channel, for performing location registration for use of a broadcast service, decrypting the broadcast data using the predetermined encryption information transmitted via the base station while using the broadcast service, generating a registration identifier as identification information of the encryption information, and transmitting the generated registration identifier to the base station"
- "at least one base station for transmitting to the mobile station broadcast data transmitted via the packet data service node while the mobile station is using the broadcast service, receiving a predetermined registration message transmitted during location registration of the mobile station, analyzing a registration identifier of the predetermined encryption information included in the registration message, and determining whether to update the predetermined encryption information for the mobile station according to the analysis result"

however, Jobst et al do disclose,

- "This request message 36 is forwarded from the phone 1 via the air and a base station 32 in the communication network to a software provider 33 authorized by the manufacturer of the phone" [column 7 lines 5-8];
- "a base station 32 in the communication network to a software provider 33 authorized by the manufacturer of the phone" [column 7 lines 5-8];

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include, "at least one mobile station connected to the base station through the radio channel, for performing location registration for use of a broadcast service, decrypting the broadcast data using the predetermined encryption information transmitted via the base station while using the broadcast service, generating a registration identifier as identification information of the encryption information, and transmitting the generated registration identifier to the base station" and "at least one base station for transmitting to the mobile station broadcast data transmitted via the packet data service node while the mobile station is using the broadcast service, receiving a predetermined registration message transmitted during location registration of the mobile station, analyzing a registration identifier of the predetermined encryption information included in the registration message, and determining whether to update the predetermined encryption information for the mobile station according to the analysis result," in the invention as disclosed by Jobst et al since it is necessary to have at least one mobile station and at least one base station in a communications network in order to have any type of operable system with procedures for authentication and encryption.

Claim 32:

Jobst et al disclose, a broadcast service system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 31 above, further comprising,

- "the registration identifier includes a hash value determined by applying a hash function to a corresponding mask key each time the mask key is updated" (i.e. "If the certification center 35 deems the request message 36 to be valid the certification center 35 then calculates a phone password 40. According to the preferred embodiment the phone password 40 may be calculated by means of a per se known secure hash algorithm") [column 7 lines 24-28].

Claim 33:

Jobst et al disclose, a broadcast service system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 31 above, further comprising,

- "the registration identifier includes a sequence number sequentially assigned to a corresponding mask key each time the mask key is updated" (i.e. "The output from the signature generating algorithm 42 may be regarded as a first digital signature 43 (sig2)

that is unique for the this specific software transfer, as it is based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code") [column 7 lines 48-52].

Claim 34:

Jobst et al disclose, a broadcast service system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 31 above, further comprising,

- "the base station performs an accounting process on the mobile station through the packet data service node when the base station transmitted updated encryption information to the mobile station" (i.e. "requesting communication terminal transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code identifying the requesting communication terminal; said providing communication terminal verifies the validity of the first unique identification code, and upon a successful verification, responds by transferring a message to the requesting communication terminal including the requested data packet and a second unique identification code; and said requesting communication terminal verifies the validity of the second unique identification code, and upon a successful verification, stores the data packet accordingly") [column 1 lines 55-67].

Claim 35:

Jobst et al disclose, a broadcast service system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 31 above, further comprising,

- "the base station receives a registration message including a predetermined mask key request bit for requesting transmission of the mask key from the mobile station while the mobile station is using a broadcast service, and transmitting predetermined encryption information including the mask key and lifetime information of the mask key to the mobile station if the mask key request bit has a predetermined bit value" (i.e. "requesting communication terminal transfers a message to the providing communication terminal including a request for receiving the data packet and a first unique identification code identifying the requesting communication terminal; said providing communication terminal verifies the validity of the first unique identification code, and upon a successful verification, responds by transferring a message to the requesting communication terminal including the requested data packet and a second unique identification code; and said requesting communication terminal verifies the validity of the second unique identification code, and upon a successful verification, stores the data packet accordingly") [column 1 lines 55-67].

Claim 36:

Jobst et al disclose, a broadcast service system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is encrypted with predetermined encryption information and provided to the mobile station, as in Claim 31 above, further comprising,

- "the encryption information can be used for decryption of the broadcast data only for a predetermined lifetime, wherein the base station transmits to the mobile station both current encryption information and next encryption information including their lifetimes if it is determined that a registration message of the mobile station was received within a predetermined skew time before a lifetime of current encryption information expires, wherein the mobile station decrypts the broadcast data using the next encryption information when the lifetime of the current encryption information expires" (i.e. " When the certification center 35 has calculated the first digital signature 43 (sig2) the service provider 33 starts to transfer the binary code 44 (the code image) of the file and the calculated first digital signature 43 (sig2) to the requesting phone... When the phone 1 receives a binary code 47 and the first digital signature 43 (16 bytes) it extracts these two parts from the message based on the information included in the header of the message 41. Apart from the IMEI code 37 the phone password 45 is stored as a part of the MT software 30 in the phone... Based on the binary code 47 (the code image) and the phone password 45 the phone 1 starts to calculate a second signature 46 (sig2'). The stored Phone Password 45 is put into the beginning and the end of a binary string having the

binary code 47 (the code image) of the file received in the middle, For this purpose the binary string is inputted to the very same signature generating algorithm 42 as used by the software provider 33 for calculating the first signature 43 (sig2). When the second signature 46 has been calculated the phone 1 compares this calculated second signature 46 with the first signature 43 received by the response message...If these two signatures 43 and 46 fit together that is are identical the phone 1 deems the response message to be coming from an authorized software provider having access to the Master Password 38. Therefor the phone 1 deems the received code image to be authentic and starts to transfer the down loaded code 31 to the MT software...When the two signatures 43 and 46 are different this may be caused by errors in the transmission. Then steps 201-208 are repeated. If the re-transmission is also unsuccessful the phone may automatically inform the service provider about the situation and desist from further attempts") [columns 7, 8, & 11].

Response to Arguments

6. Applicant's arguments filed 09-04-2007 have been fully considered but they are not persuasive.

Regarding Claims 17, 19, 20, 22, & 24:

- The applicant's argument that, "Jobst does not disclose encryption information including a predetermined mask key and lifetime information of the corresponding predetermined mask key," has been considered, however, the examiner disagrees. As stated in the 35 U.S.C. 103(a) rejection above, Jobst does not explicitly disclose "a predetermined mask

key and lifetime information of the corresponding predetermined mask key," however, Jobst does disclose "a request for receiving the data packet and a first unique identification code." It is implied and reasonable to expect that a first unique identification code may be used similar to "a predetermined mask key" where "lifetime information" would be included in the request for receiving the data packet.

Regarding Claims 20, 22, & 24:

- The applicant's argument that, "Jobst does not disclose receiving/transmitting both current encryption information and next encryption information," however, the examiner disagrees. As stated in the 35 U.S.C. 103(a) rejection above, Jobst does not explicitly recite, "receiving/transmitting both current encryption information and next encryption information," however, Jobst does disclose, "said providing communication terminal verifies the validity of the first unique identification code, and upon a successful verification, responds by transferring a message to the requesting communication terminal including the requested data packet and a second unique identification code; and said requesting communication terminal verifies the validity of the second unique identification code" [column 1 lines 59-67].

The examiner notes that although the applicant's invention may deal with, "an update in case a transmitted registration identifier is different from a currently valid registration identifier," the method is also applicable to authentication.

Conclusion

7. Applicant's arguments filed 09/04/2007 have been fully considered but they are not persuasive.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL

10/29/2007

Nasser Moazzami

Supervisory Patent Examiner

10/29/07